IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

| | | |
|---|---|---|
| UNITED STATES OF AMERICA | : | |
| | : | |
| | : | |
| | : | |
| | : | |
| | : | CRIMINAL ACTION NO. |
| | : | 1:20-cr-00126-LMM-JSA-1 |
| v. | : | |
| | : | |
| | : | |
| THOMAS ADDAQUAY | : | |
| | : | |
| | : | |
| | : | |
| | : | |

**ORDER**

This case comes before the Court on the Magistrate Judge's Report and Recommendation [78] recommending that Defendant Thomas Addaquay's Motion to Suppress [64] be denied. After due consideration, the Court enters the following Order:

## I. BACKGROUND

On June 29, 2017 the Government applied for a warrant to seize and search the contents of Defendant's email account (the "Target Account"). The Government supported its application with an affidavit from Special Agent Ira Singleton of the Internal Revenue Service ("IRS"). The Government asserted there was probable cause to believe Defendant had violated several statutes prohibiting identity theft, wire fraud, theft of government funds, and money

laundering, and that the Target Account "was used in furtherance of" the commission of these crimes. Dkt. No. [64-1] at 13.

According to Special Agent Singleton's affidavit, a company named Reliafund, Inc. ("Reliafund") processed income tax refund checks for United Consolidated Accounting and Business Services, Inc. ("United Consolidated"), an entity Defendant controlled. Id. at 14. Based on copies of refund checks and records of wire transfers, from July 30, 2013 to June 30, 2015, the affidavit claims that Reliafund wired more than $14 million to bank accounts Defendant controlled. Id. at 15. Special Agent Singleton's affidavit testimony connected these accounts with Defendant through information from bank statements, bank records, and communications between Reliafund and Defendant. Id. at 16–17. The affidavit lists the specific accounts involved and explicitly states that the transferred funds derive from federal income tax refunds. Id. Special Agent Singleton avers that the taxpayers to whom the IRS issued refunds "were unaware" that tax returns had been filed in their names. Id. at 15. Agents interviewed "[s]ome" of these individuals; "[m]any" filed identity theft affidavits with the IRS, and "none" knew how their identities were used to file tax returns. Id. at 16. On June 30, 2015, Reliafund suspended United Consolidated's account because it claimed that United Consolidated had submitted checks outside its market area. Id. at 18.

On June 29, 2017, a United States Magistrate Judge granted the Government's warrant application. The warrant set out a two-step seizure-and-

search procedure. First, Google, Inc. ("Google"), which hosted Defendant's email account, would turn over essentially all communications and identifying information associated with the account—for example, emails, instant messages, metadata pertaining to those communications, IP addresses used to log in to the account, the name and address of the account owner, and the account's web browsing history. Id. at 3–4. Second, the Government would cull Google's disclosure for several categories of information relevant to the crimes for which probable cause existed. See id. at 4–5. The Magistrate Judge allowed the Government two weeks to execute the warrant on Google, id. at 1, but did not give the Government a deadline for completing the warrant's second step or limit the Government's ability to retain the information Google provided.

On March 10, 2020, a grand jury returned an indictment charging Defendant and two others with wire fraud, conspiracy to commit wire fraud, aggravated identity theft, money laundering, and conspiracy to commit money laundering. See Dkt. No. [1]. On December 4, 2020, Defendant filed the instant Motion to Suppress evidence obtained pursuant to the June 29, 2017 warrant. Dkt. No. [64]. He argued that the warrant was unsupported by probable cause, based on stale information, overbroad, and insufficiently particularized. Id. at 10–19. He also claimed that the Government executed the warrant unreasonably by failing to timely review Google's production and to segregate information protected by the attorney-client privilege. Id. at 19–25. After full briefing, the

Magistrate Judge recommended that Defendant's Motion be denied. Dkt. No. [78].

Defendant now objects to the Magistrate Judge's findings as to probable cause, Special Agent Singleton's good faith, overbreadth, lack of particularity, and unreasonable execution.[1] See Dkt. No. [82] at 1–2. The Government has not responded to Defendant's objections, and the matter is now ripe for the Court's review.

## II. LEGAL STANDARD

Under 28 U.S.C. § 636(b)(1), the Court reviews the Magistrate Judge's Report and Recommendation for clear error if no objections are filed. 28 U.S.C. § 636(b)(1). If a party files objections, the district court must review *de novo* any part of the Magistrate Judge's disposition that is the subject of a proper objection. Id. As Defendant has filed objections to the Magistrate Judge's findings, the Court reviews the challenged findings and recommendations on a *de novo* basis.

## III. DISCUSSION

### A. Probable Cause

According to Defendant, numerous purported deficiencies in Special Agent Singleton's affidavit preclude a finding of probable cause. Specifically, he says the affidavit does not quantify (i) how many people said tax returns were filed without authorization on their behalf, (ii) "exactly how many checks were

[1] Defendant does not object to the Magistrate Judge's conclusion that the warrant was not based on stale information, and the Court notes its agreement with the Magistrate Judge's sound reasoning on this point.

processed through Reliafund," or (iii) "the amount of fraudulent transactions in comparison to the" $14 million figure given by Special Agent Singleton. Dkt. No. [82] at 3. Defendant also argues that the affidavit does not make clear the number of allegedly defrauded individuals with whom investigators spoke. Id. After careful review, the Court agrees with the Magistrate Judge that the affidavit amply supports a finding of probable cause.

"Probable cause exists when under the totality-of-the-circumstances there is a fair probability that contraband or evidence of a crime will be found in a particular place." United States v. Tobin, 923 F.2d 1506, 1510 (11th Cir. 1991) (alteration omitted) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)). "For an officer's affidavit to support probable cause, it cannot be 'a mere conclusory statement that gives the magistrate judge virtually no basis at all for making judgment regarding probable cause,' but rather 'must provide the magistrate judge with a substantial basis for making that judgment.'" United States v. James, 601 F. App'x 789, 791–92 (11th Cir. 2015) (quoting Gates, 462 U.S. at 239). Using information from bank statements and bank records, the affidavit traces more than $14 million in wire transfers to bank accounts Defendant controlled. Dkt. No. [64-1] at 15–16. Special Agent Singleton explicitly links this dollar amount to illicitly acquired income tax refunds, writing that these "funds stemmed from federal income tax refunds . . . in the names of taxpayers who were unaware of the tax return filings." Id. at 15. The affidavit does not refer to the number of *checks* "processed through Reliafund," Dkt. No. [82] at 3, but traces Defendant's

alleged proceeds to exactly 251 wire transfers, Dkt. No. [64-1] at 16. Though the affidavit does not state the precise number of taxpayers with whom investigators spoke, it is clear that each of these taxpayers was unaware that a return had been filed in their name. Taken together and viewed in "a realistic and commonsense" light, this information provides a substantial basis for the Magistrate Judge's probable cause determination. United States v. Miller, 24 F.3d 1357, 1361 (11th Cir. 1994); see United States v. Robinson, 62 F.3d 1325, 1331 n.9 (11th Cir. 1995) ("Opinions and conclusions of an experienced agent regarding a set of facts are properly a factor in the probable cause equation for issuing a search warrant." (alterations and internal quotation marks omitted) (quoting United States v. Motz, 936 F.2d 1021, 1024 (9th Cir. 1991))).

Defendant says the fact that he operated a check-cashing business explains the pattern of transactions at issue. Dkt. No. [82] at 4. But probable cause does not require the degree of certainty Defendant demands. In addition to all the information described above, Special Agent Singleton pointed out that Reliafund suspended United Consolidated's account because United Consolidated had been submitting checks bearing addresses outside its market area. Dkt. No. [64-1] at 18. Additionally, contact information associated with the Target Account and communications disclosed by Reliafund provide ample evidence that Defendant used the Target Account to correspond with Reliafund about check processing and wire transfers. See id. at 17. The affidavit may not *prove* that Defendant routed illicitly acquired income tax refunds through Reliafund but, taken as a

whole, the statements sworn to by Special Agent Singleton show at least a "fair probability" that the Target Account contains evidence of identity theft, wire fraud, theft of government funds, and money laundering. Thus, the Magistrate Judge's probable cause determination was proper, and Defendant's objection that Special Agent Singleton's affidavit failed to establish probable cause is **OVERRULED**.

**B. Good Faith Exception**

Although Defendant did not raise it in his Motion to Suppress, there is an exception to the Fourth Amendment's probable cause requirement when law enforcement officers "act[] in reasonable reliance upon a search warrant that is ultimately found to be unsupported by probable cause." United States v. Martin, 297 F.3d 1308, 1313 (11th Cir. 2002) (citing United States v. Leon, 468 U.S. 897, 922 (1984)). In his Report and Recommendation, the Magistrate Judge reasoned that even if the warrant was not supported by probable cause, "the facts in the affidavit . . . presented a more than reasonable basis" to believe that probable cause existed. Dkt. No. [78] at 6. Defendant objects that the affidavit "misled" the Magistrate Judge who signed the warrant because Agent Singleton "purposefully omit[ed] critical information which he knew was relevant and could defeat a finding of probable cause . . . ." Dkt. No. [82] at 6–7.

Defendant refers to one of four situations in which Leon's good faith exception does not apply: "where 'the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would

have known was false except for his reckless disregard of the truth . . . .'" Martin, 297 F.3d at 1313 (quoting Leon, 468 U.S. at 923). "To justify suppression of evidence" under this rule, "the alleged deliberate or reckless failure to include material information in the affidavit must conceal information that would defeat probable cause." United States v. Steiger, 318 F.3d 1039, 1046 (11th Cir. 2003). Thus, it must be true that (i) probable cause would not have existed if Special Agent Singleton had included certain information in his affidavit, and (ii) Special Agent Singleton knowingly or recklessly omitted that information.

Defendant asserts that the affidavit fails to say whether he examined the source of the tax refund checks at issue and omits the fact that Defendant used check-processing services because he ran a check-cashing business. Dkt. No. [82] at 6–7. This does not change the probable cause calculus. The affidavit indicates that, through more than 200 wire transfers, Defendant's bank accounts received millions of dollars in funds traceable to income tax refunds addressed to taxpayers unaware of those refunds—and that the Target Account was used to correspond with the company that processed the refund checks. Defendant's operation of a check-cashing business and his personal examination of the refund checks may be relevant but, given the weight of the information in the affidavit, does not defeat probable cause.

Even if it did, the information Defendant cites is not so self-evidently important that Special Agent Singleton's failure to include it objectively shows a lack of "good faith under all the circumstances." United States v. Taxacher, 902

F.2d 867, 871 (11th Cir. 1990); see also United States v. Bridges, 347 F. App'x 459, 463 (11th Cir. 2009) (the fact that the affiant, like Special Agent Singleton, "had particular training and experience" in the subject matter of his investigation did not affect the court's analysis of objective good faith). The affidavit indicates that Special Agent Singleton conducted a reasonable investigation, and Defendant offers nothing more than speculation that Special Agent Singleton deliberately omitted any piece of information. Thus, even if the affidavit omitted information necessary to establish probable cause—which it did not—Leon's good faith exception would apply, and suppression would be inappropriate. Defendant's objection to the applicability of the good faith exception is **OVERRULED**.

### C. Overbreadth and Lack of Particularity

Defendant argued in his Motion to Suppress that the warrant is, at least functionally, the sort of "general warrant" that the Fourth Amendment is meant to prohibit. According to Defendant, the warrant's command that Google disclose essentially the entire contents of his email account, without any temporal limitation, enables the Government to rummage through a trove of his information for evidence of criminal activity. Dkt. No. [64] at 16. Although the warrant limits the Government's search to several enumerated categories of information, Defendant argued these categories are too general to meaningfully restrict the Government in practice. Id. at 19.

Analyzing these concerns under the single rubric of "Particularity," the Magistrate Judge rejected Defendant's arguments as unsupported by case law

and the facts of this case and concluded that, in any event, the good faith exception would preclude suppression. Dkt. No. [78] at 11–17. The Magistrate Judge concluded that, under United States v. Blake, 868 F.3d 960 (11th Cir. 2017), the absence of a temporal limitation on Google's disclosure does not render Defendant's warrant overbroad. And, considering other courts' approval of similar warrants and the nature of the criminal activity at issue here, the Magistrate Judge held that the warrant sufficiently particularizes the categories of information that the Government may search.

Defendant challenges those conclusions. First, he argues the Magistrate Judge misread Blake, and that suppression is required because the warrant imposes no practical subject-matter or temporal limitations on the information Google must disclose. Dkt. No. [82] at 8. Second, he argues the Magistrate Judge failed to explain why it was not possible for the warrant to include more precise descriptions of the materials the Government could search. Id. at 10. Without greater precision, he says, the Government has "unfettered discretion" to search information associated with Defendant's email account. Id. at 11.

As Defendant says, the Fourth Amendment prevents "'exploratory rummaging' . . . by 'requiring a particular description of the things to be seized.'" Blake, 868 F.3d at 973 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)). It is also true that, in dicta, Blake expressly disapproved of a warrant that authorized the seizure of "virtually every type of data that could be located in [the defendant's] Facebook account" and did not contain a temporal limitation. Id. at

966, 974. It is not true, however, that the absence of subject-matter or temporal boundaries on Google's disclosure automatically renders Defendant's warrant unconstitutionally overbroad.

Federal courts in this circuit and others, both before and after Blake, "routinely uphold warrants requiring production of all information associated with a computer hard drive or email account in the face of challenges based on the particularity requirement, so long as the warrant limits seizure to relevant evidence." United States v. Roper, No. CR 117-035, 2018 WL 1465765, at *3 (S.D. Ga. Mar. 1, 2018), adopted by 2018 WL 1463365 (S.D. Ga. Mar. 23, 2018). As the Government noted in its Response to Defendant's Motion to Suppress, this two-step procedure for seizing and searching electronically stored information is rooted in Federal Rule of Criminal Procedure 41(e)(2)(B). See Dkt. No. [73] at 10–11; see also United States v. Aboshady, 951 F.3d 1, 5 & n.2 (1st Cir. 2020) (upholding warrant seeking "all data files associated with" an email account and noting the relevance of Rule 41(e)(2)(B)). An email account, like other repositories of electronically stored information covered by Rule 41(e)(2)(B), may contain an enormous volume of data. Thus, "a warrant that requires disclosure of the entire contents of an email account and then describes a subset of that information that will be subject to seizure is reasonable" as long as its descriptors are sufficiently specific. United States v. Lee, No. 1:14-cr-227-TCB-2, 2015 WL 5567102, at *3 (N.D. Ga. Sept. 25, 2015); see also United States v. Soviravong, No. 1:19-cr-146-AT-CMS, 2019 WL 7906186, at *6 (N.D. Ga. Dec. 2, 2019) ("By

explicitly limiting the scope of what may be searched and seized to evidence of the crimes under investigation, the [warrant] was sufficiently particular to enable the searchers to reasonably ascertain and identify the documents and information authorized to be seized."), adopted by 2020 WL 709284 (N.D. Ga. Feb. 12, 2020); In re A Warrant for All Content and Other Info. Associated with the Email Acct. xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 395–96 (S.D.N.Y. 2014) [hereinafter In re Warrant] ("[W]e conclude that the warrant properly required that Google deliver all emails in the account to the Government for the purpose of allowing the Government to search the emails for items within the categories specified in the warrant.").

Defendant's warrant defines far more specifically the information the Government may search than the warrant in Blake, which allowed the Government access to all "data that 'constituted fruits, evidence and instrumentalities" of a specified crime. 868 F.3d at 967. Here, the warrant limits the Government to examining 12 categories of information—all related to tax returns, bank accounts, the acquisition of others' identities, and the people with whom Defendant's email account communicated. See Dkt. No. [64-1] at 9–11. While Defendant's warrant does not contain the ex ante limits on Google's disclosure endorsed by Blake, the clear and relevant subject-matter boundaries on the portions of that disclosure the Government may search serve to limit the Government's discretion in a way the problematic warrant in Blake did not.

That these categories may, as a whole, encompass a significant volume of information does not mean Defendant's warrant is insufficiently particular. "The prohibition of general searches is not to be confused with a demand for precise ex ante knowledge of the location and content of evidence." United States v. Richards, 659 F.3d 527, 541 (6th Cir. 2011) (quoting United States v. Meek, 366 F.3d 705, 716 (9th Cir. 2004)). This is particularly so in white-collar fraud cases such as this, which "may require the assembly of a 'paper puzzle' from a large number of seemingly innocuous pieces of individual evidence." United States v. Wuagneux, 683 F.2d 1343, 1349 (11th Cir. 1982); see also United States v. Bradley, 644 F.3d 1213, 1259 (11th Cir. 2011) ("The need for evidence is greater in complex fraud cases and justifies a more flexible reading of the particularity requirement."). A warrant must only offer a description of the physical or digital area to be searched that is "as specific as the circumstances and nature of activity under investigation permit." Wuagneux, 683 F.2d at 1349.

Here, the categories of information the warrant authorizes the Government to search are numerous but "specifically connect the items to be searched for and seized to the specific criminal conduct suspected . . . ." United States v. Zhu, 555 F. Supp. 2d 1375, 1381 (S.D. Ga. 2008). Courts routinely enforce similar warrants. See id. at 1381 & n.6 (warrant covered several categories of business records "relat[ed] to the harboring, transporting, importation and employment of unauthorized aliens"); United States v. Carroll, No. 3:15-cr-00012-TCB-RGV, 2015 WL 13741254, at *7 (N.D. Ga. Nov. 3, 2015) ("[T]he warrant authorized the

seizure of items listed in twelve categories that were specifically limited to evidence of violations of" specified statutes), adopted by 2015 WL 8491011 (N.D. Ga. Dec. 10, 2015); United States v. Hendley, No. 1:14-CR-453-ODE-JSA, 2015 WL 13736219, at *7 (N.D. Ga. Oct. 19, 2015) (warrant authorized agents to search defendant's computer for "photographs and communications" evidencing child pornography "in 'any format or media'"). Nor is there any evidence that the categories in Defendant's warrant could have been more particularly defined. In sum, the warrant "enables [a] searcher reasonably to ascertain and identify" the information within the warrant's scope. United States v. Santarelli, 778 F.2d 609, 614 (11th Cir. 1985). Thus, it is sufficiently particular.

Moreover, the good faith exception would require the denial of Defendant's Motion even if the warrant was overbroad or lacked particularity.[2] As the Magistrate Judge noted and as the above analysis shows, this Court and other courts in this circuit have approved warrants with similar two-step procedures and categorical subject-matter limitations. Dkt. No. [78] at 17. Thus, assuming Defendant's warrant does not hew to the standards set in those cases, it is not "so facially deficient . . . that the executing officers cannot reasonably presume it to be valid." Leon, 468 U.S. at 923. Defendant's objections to the Magistrate Judge's conclusions as to the warrant's breadth and particularity are **OVERRULED**.

[2] That exception applies to overbreadth and particularity just as it does to probable cause. See United States v. Travers, 233 F.3d 1327, 1330 (11th Cir. 2000) (overbreadth); United States v. Accardo, 749 F.2d 1477, 1481 (11th Cir. 1985) (particularity).

### D. The Government's Execution of the Warrant

Defendant argued in his Motion to Suppress that, notwithstanding the issues discussed above, the evidence derived from the warrant should be suppressed because the Government has unreasonably delayed its review of Google's production and has failed to isolate information subject to the attorney-client privilege. Dkt. No. [64] at 19–25. The Magistrate Judge concluded that even if the Government has not yet reviewed the information Google disclosed, its failure to do so would not violate Rule 41, the Fourth Amendment, or the terms of the warrant. Dkt. No. [78] at 19. And while the Magistrate Judge reminded the Government to "take great care" when handling potentially privileged information, he held that the Court need not prescribe search terms or other protective measures ex ante. Id. at 24.

Defendant again says the Government's retention of his data is unreasonable because the Government has not yet begun its review. Dkt. No. [82] at 12. The Government has indeed been investigating Defendant for several years. However, as this Court held in a similar case, "the fact that the Government cannot indefinitely retain [a defendant's] e-mails 'for use in future criminal investigations' does not mean that it has acted unlawfully or unreasonably in retaining that information during the pendency of" a defendant's case. Lee, 2015 WL 5667102, at *4 (quoting United States v. Ganias, 755 F.3d 125, 137 (2d Cir. 2014)). "[T]he Government has a need to retain materials as an investigation unfolds for the purpose of retrieving material that is authorized by the warrant."

In re Warrant, 33 F. Supp. 3d at 398. Recognizing this reality, Rule 41 does not prescribe an "arbitrar[y] . . . presumptive time period for the return of electronically stored information." Fed. R. Crim. P. 41(e)(2) advisory committee's note to 2009 amendments. This Court will not impose such a limit when Defendant's case remains pending.

The Court's conclusion might be different if this was "a case where the Government has been shown to have abandoned the original investigatory purposes of the warrant and begun an entirely new, warrantless search for other non-authorized types of evidence." Dkt. No. [78] at 20 (citing United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999)). As the Magistrate Judge correctly noted, this is not such a case. Defendant offers only speculation in rebuttal. First, he claims his indictment and the warrant do not allege exactly the same violations of law. Dkt. No. [82] at 12. This hardly suggests a fishing expedition because the conduct underlying both is the same; the indictment covers the same time period as the warrant and likewise alleges that Defendant fraudulently obtained income tax refunds in the names of taxpayers whose identities had been stolen. Second, he says "it is at least plausible" that the Government has used the information disclosed by Google in connection with a second indictment against him. Id. However, Defendant offers no evidence that the Government has warrantlessly searched the information it obtained, and the Court is in no position to speculate. While Defendant may be dissatisfied with the pace of the Government's investigation, there is no reason to believe the Government has

"unreasonably or unlawfully" handled the information it received pursuant to the warrant. Lee, 2015 WL 5667102, at *4.

Finally, Defendant rejects the Magistrate Judge's conclusion that the warrant need not provide for the segregation of privileged communications. Defendant argues that the Government must designate a team unconnected with this case to review his emails for privilege, and that if the Government does not do so it "should be required to prove" that all its evidence came from a source other than the warrant. Dkt. No. [82] at 13–14.

Defendant points to no authority requiring the Court to impose any review procedures on the Government. To the contrary, Eleventh Circuit precedent indicates that the Court may leave the Government to devise its own search methods and review the reasonableness of those methods ex post. See United States v. Khanani, 502 F.3d 1281, 1290–91 (11th Cir. 2007) (holding that protocols the Government designed constituted reasonable measures to cabin a search to a warrant's scope). Given the complex and indeterminate nature of criminal investigations, many courts take the same approach and decline to impose search protocols or procedures on the Government before the Government conducts its search. See Richards, 659 F.3d at 538 & n.6 (collecting cases); see also United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009) (explaining the rationale for the court's reluctance to "limit computer searches" in advance). In short, precedent does not require courts to "[j]udg[e] the reasonableness of the execution of a search ex ante . . . ." In re Warrant, 33

F. Supp. 3d at 396. Instead, the Court may assess the reasonableness of the Government's search ex post and order suppression, among other remedies, if the Government unreasonably exceeds the scope of the warrant. The threat of suppression serves to deter the intrusion Defendant fears. See United States v. Herring, 492 F.3d 1212, 1217 (11th Cir. 2007) (discussing the exclusionary rule's role in deterring Government misconduct). At this point, the Court declines to prescribe a search procedure for the Government to follow. Defendant's objections to the reasonableness of the Government's execution of the warrant are **OVERRULED**.

## IV. CONCLUSION

In light of the foregoing, the Court **ADOPTS** the Magistrate Judge's Report and Recommendation [78] as the opinion of this Court. Defendant's objections are **OVERRULED**. Defendant's Motion to Suppress [64] is **DENIED**.

**IT IS SO ORDERED** this 19th day of April, 2021.

**Leigh Martin May**
**United States District Judge**